



Proyecto Final de Módulo

Diseño y Evaluación de Seguridad Básica en una Aplicación Web Simulada

Objetivo General:

Aplicar conocimientos fundamentales sobre **autenticación, autorización, gestión de sesiones, criptografía básica y OWASP Top 10**, a través del análisis y propuesta de mejoras de una aplicación web simulada.

Escenario Simulado:

Has sido contratado como asesor junior en ciberseguridad por una empresa ficticia llamada **SafeStart**, que tiene una aplicación web interna para gestión de empleados. Esta app tiene problemas de seguridad básica y necesita tu ayuda para identificar riesgos y proponer soluciones prácticas.

La aplicación presenta las siguientes características iniciales:

- Tiene un formulario de login basado solo en usuario y contraseña.
 - Las contraseñas se guardan en texto plano.
 - No utiliza sesiones expiran ni cookies seguras.
 - Todos los usuarios acceden al mismo panel, sin distinción de roles.
 - No hay registro de accesos ni alertas de actividad sospechosa.
-

Tareas del Proyecto:

1. Análisis de Autenticación:

- Explica qué debilidades existen en el sistema de login.
- Sugiere una mejora de autenticación con al menos **dos factores de seguridad**.
- Menciona al menos **un protocolo moderno recomendado** para manejar la autenticación.

2. Propuesta de Autorización:

- Diseña una tabla con **tres tipos de usuarios** (Ej: administrador, recursos humanos, visitante).
- Describe qué permisos debería tener cada uno usando el modelo **RBAC** (control de acceso basado en roles).

3. Gestión de Sesiones:

- Describe brevemente cómo funciona una sesión web.
- Propón **dos mecanismos de protección de sesión** (por ejemplo: expiración automática, regeneración de token).
- Explica cómo se usaría **una cookie segura** en este caso.

4. Seguridad Criptográfica:

- Menciona cómo deberían almacenarse correctamente las contraseñas (ej: algoritmo recomendado).
- Describe brevemente la diferencia entre **hashing** y **cifrado**.

5. Análisis OWASP Top 10:







- Elige **3 vulnerabilidades del OWASP Top 10** que podrían estar presentes en la app.
- Para cada una:
 - Explica en qué consiste la vulnerabilidad.
 - Describe cómo se podría mitigar.

6. Herramientas de Evaluación:

- Menciona **una herramienta gratuita** que podrías usar para analizar la seguridad de esta app (como OWASP ZAP).
 - Describe brevemente cómo se usaría para detectar fallos básicos.
-

Paso 7: Informe Técnico de Evaluación de Seguridad

El informe final debe incluir:

-  **Diagnóstico de Seguridad Actual:** resumen de las vulnerabilidades encontradas en autenticación, sesiones, permisos, criptografía y OWASP.
-  **Propuesta de Mejora:** explicaciones claras y justificadas de cada recomendación aplicada.
-  **Modelo de Roles y Permisos (RBAC):** tabla con roles y accesos diferenciados.
-  **Resumen Criptográfico:** algoritmos sugeridos y distinción entre técnicas.
-  **Pruebas Realizadas:** evidencia de evaluación (pantallas, comandos, pruebas funcionales si se usó ZAP o similar).
-  **Reflexión profesional** (ver paso 8).

Producto entregable:

`informe_seguridad_safestart.pdf` o `informe_seguridad_safestart.docx`
con marca de agua: "Auditoría de Seguridad – SafeStart App Simulada".

Paso 8: Reflexión Ética y Profesional







Incluye una sección final titulada "*Reflexión Ética y Profesional*" con 5 a 10 líneas que responda:

- ¿Qué importancia tiene proteger desde el inicio las funciones básicas como login y roles?
 - ¿Cómo impacta la mala gestión de sesiones en la seguridad real de una empresa?
 - ¿Qué decisiones tomaste que reflejan buenas prácticas en ciberseguridad?
 - ¿Qué aprendiste sobre el equilibrio entre facilidad de uso y seguridad en entornos reales?
-

Criterios de Evaluación (máximo 10 puntos)

Criterio	Puntaje
Análisis correcto de debilidades y riesgos	2 pts
Propuestas realistas y técnicas de mejora	2 pts
Aplicación clara del modelo de roles (RBAC)	1.5 pts
Gestión adecuada de sesiones y cookies	1.5 pts
Enfoque criptográfico preciso y justificado	1 pt
Evaluación OWASP y uso de herramientas adecuadas	1 pt
Informe profesional y reflexión ética incluida	1 pt

Recursos Recomendados

-  [OWASP ZAP](#) – Análisis de aplicaciones web
 -  [OWASP Top 10](#) – Guía oficial de vulnerabilidades
 -  [Auth0 - Password Storage Cheat Sheet](#)
 -  OWASP Cheat Sheets (Session Management, Authentication, Access Control)
 -  [JWT.io](#) – Para comprender y probar tokens
 -  Ciberseguridad para desarrolladores (Google, Coursera, Udemy)
-

Reflexión Final

“La seguridad en una aplicación web no comienza cuando algo falla, sino desde el diseño. Comprender cómo proteger el login, definir roles con claridad y cuidar la sesión del usuario es el primer paso hacia una aplicación profesional. Las soluciones simples pero bien pensadas pueden prevenir brechas graves. Evaluar riesgos no es solo técnica, es responsabilidad.”
